CLAIMS:

1. A system for facilitating a cooperative response by a plurality of members of a domain to a threat condition, with each of the plurality of members being operable to generate log records, the system comprising:

a log server operable to receive and store the log and audit records;

a detection server operable to access the log server and parse the stored log and audit records in identifying an occurrence of the threat condition; and

a profile server operable to store an alert status indicative of identification of the occurrence of the threat condition by the detection server,

wherein each of the plurality of members is operable to query the profile server in order to check an alert status, and, in response to an alert, to implement a pre-defined action.

2. The system as set forth in claim 1, wherein the domain is defined as a logical grouping of the plurality of members which are not necessarily otherwise related.

3. The system as set forth in claim 2, wherein the logical grouping is based upon a value characteristic and a risk tolerance characteristic of each of the plurality of members.

4. The system as set forth in claim 1, wherein the detection server applies a threat-detection logic in conjunction with a pre-established threshold value in identifying the occurrence of the threat condition.

5. The system as set forth in claim 1, wherein the profile server is operable to provide a security profile including -

a log server IP address operable to identify the log server to which each of the plurality of members should send the log records;

a configuration refresh frequency operable to a define a frequency at which to query the profile server for an update of the security profile;

a device value operable to define a value of each of the plurality of members, wherein the device value is used by the detection server when identifying the occurrence of the threat condition;

a threshold value operable in conjunction with a threat detection logic used by the detection server in identifying the occurrence of the threat condition; and

an alert query frequency operable to define a frequency at which to query the profile server for an update of the alert status.

6. The system as set forth in claim 1, wherein the alert automatically expires, if no additional action is taken, after a pre-defined period of time.

7. The system as set forth in claim 1, wherein the plurality of members are operable to send via a non-routable protocol a broadcast message communicating the occurrence of the threat condition to an edge device.

8. The system as set forth in claim 1, wherein the occurrence of the threat condition is communicated to a second domain for evaluation and possible pre-emptive action.

9. A system for facilitating a cooperative response by a plurality of members of a domain to a threat condition, with each of the plurality of members being operable to generate log records, the system comprising:

a log server operable to receive and store the log and audit records;

a detection server operable to access the log server and parse the stored log and audit records in identifying an occurrence of the threat condition;

a profile server operable to store an alert status indicative of identification of the occurrence of the threat condition by the detection server, wherein each of the plurality of members are operable to query the profile server in order to check the alert status, and, in response to an alert, to implement a pre-defined response, and further operable to send via a non-routable protocol a broadcast message communicating the occurrence of the threat condition to an edge device; and

a protective firewall interposed between the domain and the log server, detection server, and profile server

10. The system as set forth in claim 9, wherein the domain is defined as a logical grouping of the plurality of members which are not necessarily otherwise related.

11. The system as set forth in claim 10, wherein the logical grouping is based upon a value characteristic and a risk tolerance characteristic of each of the plurality of members.

12. The system as set forth in claim 9, wherein the detection server applies a threat-detection logic in conjunction with a pre-established threshold value in identifying the occurrence of the threat condition.

13. The system as set forth in claim 9, wherein the profile server is operable to provide a security profile including -

a log server IP address operable to identify the log server to which each of the plurality of members should send the log records;

a configuration refresh frequency operable to a define a frequency at which to query the profile server for an update of the security profile;

a device value operable to define a value of each of the plurality of members, wherein the device value is used by the detection server in identifying the occurrence of the threat condition;

a threshold value operable in conjunction with a threat detection logic used by the detection server in identifying the occurrence of the threat condition; and

an alert query frequency operable to define a frequency at which to query the profile server for an update of the alert status.

14. The system as set forth in claim 9, wherein the alert automatically expires, if no additional action is taken, after a pre-defined period of time.

15. The system as set forth in claim 9, wherein the occurrence of the threat condition is communicated to a second domain for evaluation and possible pre-emptive action.

16. A computer program for facilitating a cooperative response by a plurality of members of a domain to a detected threat condition, with each of the plurality of members being operable to generate log records, the computer program comprising:

a code segment operable to copy the log records to a remote location;

a code segment operable to receive and store the log records;

a code segment operable to parse the stored log records in identifying an occurrence of the threat condition;

a code segment operable to set an alert status indicative of identification of the occurrence of the threat condition; and

a code segment operable to periodically query the alert status, and, in response to an alert, to implement a pre-defined action.

17. The computer program as set forth in claim 16, wherein the domain is defined as a logical grouping of the plurality of members which are not necessarily otherwise related.

18. The computer program as set forth in claim 17, wherein the logical grouping is based upon a value characteristic and a risk tolerance characteristic of each of the plurality of members.

19. The computer program as set forth in claim 16, wherein the detection server applies a threat-detection logic in conjunction with a pre-established threshold value in identifying the occurrence of the threat condition.

20. The computer program as set forth in claim 16, further comprising a code segment operable to provide to the plurality of members a security profile including -

a log server IP address operable to identify the remote location to which the log records are to be copied;

a configuration refresh frequency operable to a define a frequency at which the security profile should be queried;

a device value operable to define the value of the plurality of members, wherein the device value is used in identifying the occurrence of the threat condition;

a threshold value operable to define a logic to be used in identifying the occurrence of the threat condition; and

an alert query frequency operable to define a frequency at which to query the alert status.

21. The computer program as set forth in claim 16, wherein the alert automatically expires, if no additional action is taken, after a pre-defined period of time.

22. The computer program as set forth in claim 16, further including a code segment operable to send via a non-routable protocol a broadcast message to an edge device communicating the occurrence of the threat condition.

23. The computer program as set forth in claim 16, further including a code segment operable to communicate the occurrence of the threat condition to a second domain for evaluation and possible pre-emptive action.

24. A method of facilitating a cooperative response by a plurality of members of a domain to a threat condition, with each of the plurality of members being operable to generate log records, the method comprising the steps of:

(a) receiving and storing copies of the log records in a remote location;

(b) parsing the stored log records in identifying an occurrence of the threat condition;

(c) setting an alert status indicative of identification of the occurrence of the threat condition; and

(d) allowing the plurality of members to periodically query the alert status, and, in response to an alert, to implement a pre-defined action.

25. The method as set forth in claim 24, wherein the domain is defined as a logical grouping of the plurality of members which are not necessarily otherwise related.

26. The method as set forth in claim 25, wherein the logical grouping is based upon a value characteristic and a risk tolerance characteristic of each of the plurality of members.

27. The method as set forth in claim 24, wherein the occurrence of the threat condition is identified by use of a threat-detection logic in conjunction with a pre-established threshold value.

28. The method as set forth in claim 24, further comprising the step of (e) providing to the plurality of members a security profile including -

a log server IP address operable to identify the remote location to which the log records are to be copied;

a configuration refresh frequency operable to a define a frequency at which the security profile should be queried;

a device value operable to define the value of the plurality of members, wherein the device value is used in identifying the occurrence of the threat condition;

a threshold value operable to define a logic to be used in identifying the occurrence of the threat condition; and

an alert query frequency operable to define a frequency at which to query the alert status.

29. The method as set forth in claim 24, further comprising the step of (e) terminating the alert automatically, if no additional action is taken, after a pre-defined period of time.

30. The method as set forth in claim 24, further including the step of (e) allowing the plurality of members to send via a non-routable protocol a broadcast message to an edge device communicating the occurrence of the threat condition.

31. The method as set forth in claim 24, further comprising the step of (e) communicating the occurrence of the threat condition to a second domain for evaluation and possible pre-emptive action.